

# Reset thresholds of automata with two cycle lengths

Vladimir V. Gusev, Elena V. Pribavkina

Institute of Mathematics and Computer Science,  
Ural Federal University, Ekaterinburg, Russia  
vl.gusev@gmail.com, elena.pribavkina@gmail.com

**Abstract.** We present several series of synchronizing automata with multiple parameters, generalizing previously known results. Let  $p$  and  $q$  be two arbitrary co-prime positive integers,  $q > p$ . We describe reset thresholds of the colorings of primitive digraphs with exactly one cycle of length  $p$  and one cycle of length  $q$ . Also, we study reset thresholds of the colorings of primitive digraphs with exactly one cycle of length  $q$  and two cycles of length  $p$ .

## 1 Introduction

A *complete deterministic finite automaton*  $\mathcal{A}$ , or simply *automaton*, is a triple  $\langle Q, \Sigma, \delta \rangle$ , where  $Q$  is a finite *set of states*,  $\Sigma$  is a finite *input alphabet*, and  $\delta : Q \times \Sigma \mapsto Q$  is a totally defined *transition function*. Following standard notation, by  $\Sigma^*$  we mean the set of all finite words over the alphabet  $\Sigma$ , including the empty word  $\varepsilon$ . The function  $\delta$  naturally extends to the free monoid  $\Sigma^*$ ; this extension is still denoted by  $\delta$ . Thus, via  $\delta$ , every word  $w \in \Sigma^*$  acts on the set  $Q$ . For each  $v \in \Sigma^*$  and each  $q \in Q$  we write  $q.v$  instead of  $\delta(q, v)$  and let  $Q.v = \{q.v \mid q \in Q\}$ .

An automaton  $\mathcal{A}$  is called *synchronizing*, if there is a word  $w \in \Sigma^*$  which brings all states of the automaton  $\mathcal{A}$  to a particular one, i.e.  $|Q.w| = 1$ . Any such word  $w$  is said to be a *reset* (or *synchronizing*) *word* for the automaton  $\mathcal{A}$ . The minimum length of reset words for  $\mathcal{A}$  is called the *reset threshold* of  $\mathcal{A}$ .

Synchronizing automata serve as transparent and natural models of error-resistant systems in many applied areas (robotics, coding theory). At the same time, synchronizing automata surprisingly arise in some parts of pure mathematics (algebra, symbolic dynamics, combinatorics on words). See recent surveys by Sandberg [10] and Volkov [13] for more details on the theory and applications of synchronizing automata.

One of the most important and natural questions related to synchronizing automata is the following: given  $n$ , how big can the reset threshold of an automaton with  $n$  states be? In 1964 Černý exhibited a series of automata with  $n$  states whose reset threshold equals  $(n-1)^2$  [4]. Soon after he conjectured, that this series represents the worst possible case, i.e. the reset threshold of every  $n$ -state synchronizing automaton is at most  $(n-1)^2$ . This hypothesis has become known

as the *Černý conjecture*. In spite of its simple formulation and many researchers' efforts, the Černý conjecture remains unresolved for about fifty years. Moreover, no upper bound of magnitude  $O(n^2)$  for the reset threshold of a synchronizing  $n$ -state automaton is known so far. The best known upper bound on the reset threshold of a synchronizing  $n$ -state automaton is the bound  $\frac{n^3-n}{6}$  found by Pin [8] in 1983.

In an attempt to understand why the Černý conjecture is so difficult to resolve, researchers started to look for *slowly synchronizing automata*, i.e. automata with  $n$  states and reset threshold close to  $(n-1)^2$ . First series of such automata were presented in [2]. The number of known series of slowly synchronizing automata was significantly increased in [1]. In the latter paper the constructions are based on the observed connection between slowly synchronizing automata and primitive digraphs with large exponent.

A digraph  $D$  is said to be *primitive*, if there is a positive integer  $t$  such that for every pair of vertices  $u$  and  $v$  there is a path from  $u$  to  $v$  of length  $t$ . The smallest  $t$  with this property is called the *exponent* of the digraph  $D$ . Equivalently, if  $M$  is the adjacency matrix of  $D$ , then  $t$  is the smallest number such that  $M^t$  is positive. For additional results on the well-established field of primitive digraphs we refer a reader to [3].

The *underlying digraph*  $\mathcal{D}(\mathcal{A})$  of an automaton  $\mathcal{A}$  has  $Q$  as the set of vertices, and  $(u, v)$  is an edge if  $u \cdot x = v$  for some letter  $x \in \Sigma$ . A *coloring* of a digraph  $D$  is an automaton  $\mathcal{A}$  such that  $\mathcal{D}(\mathcal{A})$  is isomorphic to  $D$ . Proposition 2 [1] states, that the reset threshold of an arbitrary  $n$ -state strongly connected synchronizing automaton is greater than the exponent of the underlying digraph minus  $n$ . At the same time, the Road Coloring theorem [12] states that any primitive digraph has at least one synchronizing coloring. Thus,  $n$ -state slowly synchronizing automata can be constructed from the well-known examples [5] of primitive digraphs on  $n$  vertices with exponents close  $(n-1)^2$ . This idea was presented and explored in [1]. In the present paper we generalize several series of slowly synchronizing automata presented in [1]. Namely,  $\mathcal{W}_n$ ,  $\mathcal{D}'_n$  and  $\mathcal{D}''_n$ .

Another motivation for the present paper comes from the following facts. Computational experiments of Trahtman [11] revealed that not every positive integer in  $\{1, \dots, (n-1)^2\}$  may serve as the reset threshold of some automaton with  $n$  states over a binary alphabet. For example, there is no automaton with nine states over a binary alphabet with the reset threshold in the range from 59 to 63. Similar gaps were found for automata with the number of states ranging from 6 to 10. These results were confirmed in [1]. Moreover, a second gap was presented, i.e. there are no 9-state automata over a binary alphabet with the reset threshold from 53 to 55. For 10-state automata a third gap, along with the first two, was found in the course of computational experiments of Kisielewicz and Szykuła [6]. This brings up the following natural question: given  $n$ , which positive integers are reset thresholds of  $n$ -state automata? Surprisingly, the set  $E_n$  of all possible exponents of primitive digraphs on a fixed number  $n$  of vertices has similar gaps [5] as the set  $R_n$  of all possible reset thresholds of  $n$ -state automata. Furthermore, for every  $n$  the set  $E_n$  is fully described [3, p. 83].

We hope that study of this similarity could shed light on properties of  $R_n$ . The following statement [7] plays the key role in the description of  $E_n$ : if the exponent of a primitive digraph  $D$  is at least  $\frac{(n-1)^2+1}{2} + 2$ , then  $D$  has cycles of exactly two different lengths. This motivates our choice in the present paper to focus on automata whose underlying digraphs have exactly two different cycle lengths.

Let  $p$  and  $q$  be two arbitrary co-prime positive integers,  $q > p$ . In section 2 we describe reset thresholds of the colorings of primitive digraphs with exactly one cycle of length  $p$  and one cycle of length  $q$ . In section 3 we study reset thresholds of the colorings of primitive digraphs with exactly one cycle of length  $q$  and two cycles of length  $p$ .

## 2 Wielandt-type automata

We start with recalling the following elementary and well-known number-theoretic result.

**Theorem 1** ([9, Theorem 2.1.1]). *Given two positive co-prime integers  $p$  and  $q$ , the largest integer that is not expressible as a non-negative integer combination of  $p$  and  $q$ , is  $(p-1)(q-1) - 1$ .*

Let us fix two positive co-prime integers  $p$  and  $q$ . Without loss of generality, we assume  $p < q$ . Let  $n$  be a positive integer,  $n < p+q$ . We define a Wielandt-type automaton  $\mathcal{W}(n, q, p)$  as follows (see Fig. 2). The state set  $Q = \{0, 1, \dots, n-1\}$ ,  $\Sigma = \{a, b\}$ , and the transitions are defined in the following way:

$0 \cdot a = q$  if  $n > q$ , and  $0 \cdot a = q - p + 1$  if  $n = q$ ;  $0 \cdot b = 1$ ;  
 $i \cdot x = i + 1$  for  $1 \leq i < n - 1$  and  $i \neq q - 1$  for each  $x \in \Sigma$ ;  
 $(q - 1) \cdot x = 0$  for each  $x \in \Sigma$ ;  
 if  $n > q$ , then  $(n - 1) \cdot x = n - p + 1$  for each  $x \in \Sigma$ .

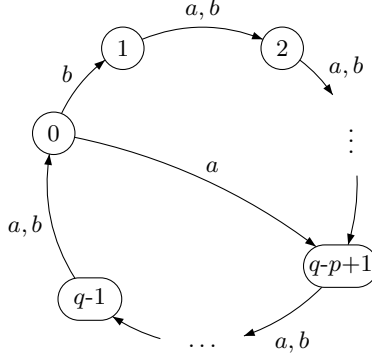
In case  $q = n$ ,  $p = n - 1$  we obtain Wielandt automaton  $\mathcal{W}_n$  considered in [1]. It is not hard to observe, that every strongly connected  $n$ -state automaton whose underlying digraph has exactly one cycle of length  $p$  and exactly one cycle of length  $q$  is isomorphic to  $\mathcal{W}(n, q, p)$ .

First let us consider the case  $n = q$  (see Fig. 1).

**Lemma 1.** *Let  $\mathcal{A}$  be a strongly connected synchronizing automaton, whose cycles have lengths  $p$  and  $q$ . If  $\gcd(p, q) = 1$ , then  $\text{rt}(\mathcal{A}) \geq (p-1)(q-1)$ . Moreover, if there are states  $s, t$ , and a positive integer  $\ell$  such that:*

- (i) *there is a shortest synchronizing word  $w$  which resets the automaton  $\mathcal{A}$  to  $s$ ,*
  - (ii)  *$t \cdot u = s$  for each word  $u$  of length  $\ell$ ,*
- then  $\text{rt}(\mathcal{A}) \geq (p-1)(q-1) + \ell$ .*

*Proof.* Let  $\mathcal{A} = \langle Q, \Sigma, \delta \rangle$ . We prove the first part of the lemma. Consider a synchronizing word  $w$  having shortest possible length. Let  $s = Q \cdot w$  be the state to which the automaton is synchronized. Note, that the word  $uw$  is synchronizing for every  $u \in \Sigma^*$ , and  $Q \cdot uw = s$ . In particular, we have  $s \cdot w = s \cdot uw = s$ . Thus the word  $w$ , as well as the word  $uw$ , for every word  $u$ , labels a path in the



**Fig. 1.** The Wielandt-type automaton  $\mathcal{W}(q, q, p)$

automaton  $\mathcal{A}$  from the state  $s$  to itself. Every such path can be decomposed into cycles of lengths  $p$  and  $q$ . Hence the number  $|w|$ , as well as  $|w| + k$ , for each positive integer  $k$ , can be represented as a non-negative combination of the numbers  $p$  and  $q$ . Thus, by theorem 1, we have  $\text{rt}(\mathcal{A}) \geq (p-1)(q-1)$ .

Assume now that in addition there exist a state  $t$  and a positive integer  $\ell$  such that  $t.u = s$  for each word  $u$  of length  $\ell$ . Suppose, contrary to our claim, that  $|w| < (p-1)(q-1) + \ell$ . Let  $u \in \Sigma^*$  be an arbitrary word such that  $|uw| = (p-1)(q-1) + \ell - 1$ . As before, the word  $uw$  synchronizes the automaton  $\mathcal{A}$  to the state  $s$ . But after applying its prefix of length  $\ell$  to the state  $t$  we end up in the state  $s$ . Hence there is a path of length  $(p-1)(q-1) - 1$  from  $s$  to itself. But this number can not be represented as a non-negative combination of  $p$  and  $q$  by theorem 1. A contradiction.

**Theorem 2.** *The reset threshold of the Wielandt-type automaton  $\mathcal{W}(q, q, p)$  equals  $(p-1)(q-1) + q - p$ .*

*Proof.* Any shortest reset word  $w$  for this automaton resets it to the state  $q-p+1$ , since it is the only state which is a common end of two different edges with the same label. Note, that any word of length  $q-p$  brings the state 1 to the state  $q-p+1$ . Lemma 1 implies that the reset threshold of  $\mathcal{W}(q, q, p)$  is at least  $(p-1)(q-1) + q - p$ .

Let us check that the word  $w = a^{q-p}(ba^{q-1})^{p-2}ba^{q-p}$  synchronizes  $\mathcal{W}(q, q, p)$ . After applying the prefix  $a^{q-p}$  we end up in the cycle  $C$  of length  $p$ :

$$Q \cdot a^{q-p} = \{0, q-p+1, q-p+2, \dots, q-1\}.$$

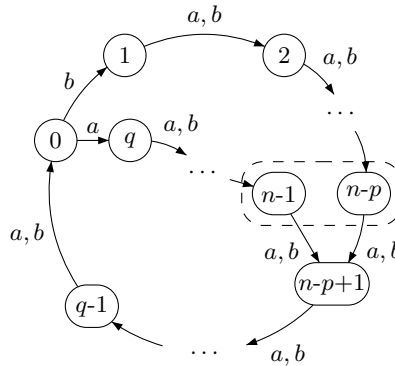
Next, we show that the word  $(ba^{q-1})^{p-2}$  brings  $C$  to a two-element set. We state this fact as a separate lemma:

**Lemma 2.** *Let  $\mathcal{A}$  be an automaton with the state set  $Q$  over the alphabet  $\Sigma = \{a, b\}$ . Let  $q > p$  be two co-prime positive integers, and let  $r$  denote the remainder of the division of  $q$  by  $p$ . Let  $C = \{0, 1, \dots, p-1\}$  be a subset of  $Q$  such that  $0.a = 1$ ,  $0.ba^{q-1} = 0$ , and  $i.x \equiv i+1 \pmod{p}$  for  $1 \leq i \leq p-1$  and for all  $x \in \Sigma$ . Then  $C \cdot (ba^{q-1})^{p-2} = \{0, p-r\}$ .*

*Proof.* First note, that  $i \cdot ba^{q-1} \equiv i + r \pmod{p}$  for each state  $i \neq 0$ . Consider the equation  $i + rx \equiv 0 \pmod{p}$ . Since  $r$  and  $p$  are co-prime, this equation has unique solution in  $\{1, \dots, p-1\}$  for every  $i \neq 0$ . Then  $i \cdot (ba^{q-1})^x = 0$ . If  $x \neq p-1$ , then  $i \cdot (ba^{q-1})^{p-2} = 0$ . The case  $x = p-1$  occurs only if  $i = r$ . In this case  $r \cdot (ba^{q-1})^{p-2} = p-r$ .

Returning back to the proof of the theorem, we have  $C \cdot (ba^{q-1})^{p-2} = \{0, q-r\}$ . The word  $ba^{q-p}$  brings the latter set to the singleton  $q-p+1$ .

Let us consider now the general case of the Wielandt-type automaton  $\mathcal{W}(n, q, p)$  (see Fig. 2). It is rather easy to see, that given a synchronizing automaton



**Fig. 2.** The Wielandt-type automaton  $\mathcal{W}(n, q, p)$

$\mathcal{B}$  and a congruence  $\rho$ , the factor automaton  $\mathcal{B}/\rho$  is also synchronizing, and  $\text{rt}(\mathcal{B}/\rho) \leq \text{rt}(\mathcal{B})$ . In particular, consider the following congruence  $\sigma$  on  $\mathcal{B}$ : for two states  $s$  and  $t$  we have  $s\sigma t$  if and only if  $s \cdot x = t \cdot x$  for each  $x \in \Sigma$ .

**Lemma 3.** *If  $\mathcal{B}$  is synchronizing, then  $\mathcal{B}/\sigma$  is also synchronizing, and*

$$\text{rt}(\mathcal{B}/\sigma) \leq \text{rt}(\mathcal{B}) \leq \text{rt}(\mathcal{B}/\sigma) + 1.$$

*Proof.* The inequality  $\text{rt}(\mathcal{B}/\rho) \leq \text{rt}(\mathcal{B})$  is trivial. The states of  $\mathcal{B}/\sigma$  are congruence classes  $[s]^\sigma$  of the states  $s$  of the automaton  $\mathcal{B}$ . Let us consider a synchronizing word  $w$  for the automaton  $\mathcal{B}/\sigma$ . For every pair of states  $s$  and  $s'$  of the original automaton  $\mathcal{B}$  we have  $s \cdot w \sigma s' \cdot w$ . But this means that  $s \cdot wx = s' \cdot wx$  for any letter  $x \in \Sigma$ , thus, the word  $wx$  resets the automaton  $\mathcal{B}$ . Thus we have  $\text{rt}(\mathcal{B}) \leq \text{rt}(\mathcal{B}/\sigma) + 1$ .

**Lemma 4.** *If  $n > q$ , then  $\mathcal{W}(n, q, p)/\sigma$  is equal to  $\mathcal{W}(n-1, q, p)$ , and*

$$\text{rt}(\mathcal{W}(n, q, p)) = \text{rt}(\mathcal{W}(n-1, q, p)) + 1.$$

*Proof.* Let  $w$  be a word of minimal length, synchronizing the automaton  $\mathcal{W}(n, q, p)$ . As in the proof of theorem 2, the word  $w$  resets  $\mathcal{W}(n, q, p)$  to the state  $n-p+1$ . On

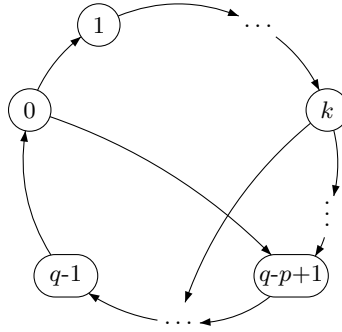
the last step  $w$  brings the states  $\{n-1, n-p\}$  to the state  $n-p+1$ . Hence  $w = w'x$ , where  $x \in \Sigma$ , and  $w'$  brings the automaton  $\mathcal{W}(n, q, p)$  to the set  $\{n-1, n-p\}$ . But these two states form the unique non-trivial  $\sigma$ -class (see Fig. 2). Thus the factor automaton  $\mathcal{W}(n, q, p)/\sigma$  is equal to the Wielandt-type automaton  $\mathcal{W}(n-1, q, p)$ . Moreover, it is synchronized by  $w'$ . Thus,  $\text{rt}(\mathcal{W}(n-1, q, p)) \leq \text{rt}(\mathcal{W}(n, q, p)) - 1$ . On the other hand, by lemma 3 we have  $\text{rt}(\mathcal{W}(n-1, q, p)) \geq \text{rt}(\mathcal{W}(n, q, p)) - 1$ . Therefore, we get the required equality.

**Theorem 3.** *The reset threshold of the Wielandt-type automaton  $\mathcal{W}(n, q, p)$  is equal to  $(p-1)(q-1) + n - p$ .*

*Proof.* Since there are  $n - q$  states on the path from the state 0 to  $n - p + 1$ , lemma 4 can be applied  $n - q$  times to obtain the Wielandt-type automaton  $\mathcal{W}(q, q, p)$ . By theorem 2, its reset threshold equals  $(p-1)(q-1) + q - p$ . Each time lemma 4 is applied, the reset threshold is decreased strictly by 1. Thus the reset threshold of the automaton  $\mathcal{W}(n, q, p)$  is equal to  $(p-1)(q-1) + n - p$ .

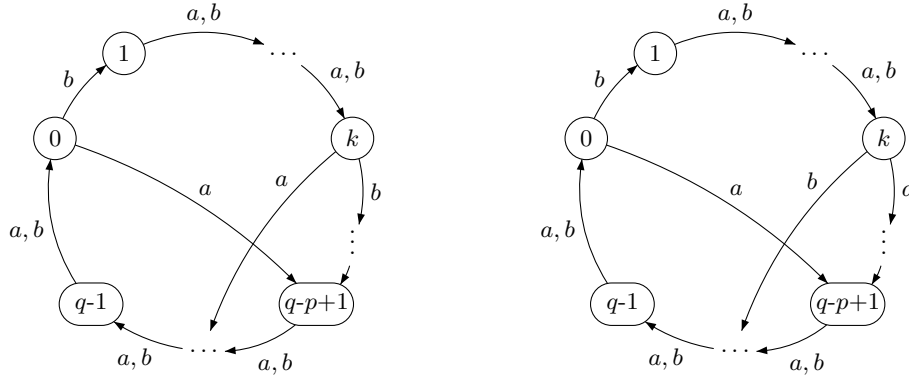
### 3 Dulmage-Mendelsohn-type automata

As in the previous section, let  $q$  and  $p$  be two co-prime positive integers, and  $q > p$ . Let  $k$  be a positive integer such that  $k < \min\{p, q-p+1\}$ . Here we consider Dulmage-Mendelsohn-type automata, which are the colorings of the following primitive digraph  $D(q, p, k)$  (see Fig. 3). Its vertex set is  $\{0, \dots, q-1\}$ , the set of edges is  $\{(i, (i+1) \bmod q) \mid 0 \leq i < q\} \cup \{(0, q-p+1), (k, (q-p+k+1) \bmod q)\}$ . Note, that  $D(q, p, k)$  has exactly one cycle of length  $q$  and two cycles of length  $p$ . The digraph  $D(q, p, k)$  has only two non-isomorphic colorings  $\mathcal{D}^{aa}(q, p, k)$  and  $\mathcal{D}^{ab}(q, p, k)$  (see Fig. 4).



**Fig. 3.** Digraph  $D(q, p, k)$

- Lemma 5.** (i) *Any shortest synchronizing word of the automaton  $\mathcal{D}^{ab}(q, p, k)$  synchronizes it to the state  $q - p + 1$ .*  
(ii) *Any shortest synchronizing word of the automaton  $\mathcal{D}^{aa}(q, p, k)$  synchronizes it to the state  $q - p + 1$  when  $k < q - p$ .*



**Fig. 4.** Two Dulmage-Mendelsohn-type automata  $\mathcal{D}^{aa}(q, p, k)$  and  $\mathcal{D}^{ab}(q, p, k)$

*Proof.* Part (i). Let  $t = q - p + k + 1$ . Note, that  $t = k \cdot b = (q - p + k) \cdot a = (q - p + k) \cdot b$ . Any shortest synchronizing word  $w$  can synchronize the automaton  $\mathcal{D}^{ab}(q, p, k)$  either to  $q - p + 1$  or  $t$ . Suppose, that  $w$  synchronizes  $\mathcal{D}^{ab}(q, p, k)$  to the state  $t$ . By lemma 1 we have  $|w| \geq (p-1)(q-1)$ . Moreover,  $(p-1)(q-1) > k$ . Consider the suffix  $v$  of  $w$  of length  $k$ . It is easy to see, that the full preimage  $t \cdot v^{-1}$  of the state  $t$  under the action of the word  $v$  is equal to  $\{1, q - p + 1\}$ . If  $k = q - p$ , then the two incoming edges to the state  $q - p + 1$  are labeled by the letter  $a$ , while the only incoming edge to the state 1 is labeled by the letter  $b$ . A contradiction. If  $k \neq q - p$ , then the set  $\{1, q - p + 1\}$  was necessarily obtained from the set  $\{0, q - p\}$  by applying the letter  $b$ . But  $\{0, q - p\} \cdot a = q - p + 1$ . Therefore, we can replace the suffix of  $w$  of length  $k + 1$  by the letter  $a$ , in order to obtain a shorter synchronizing word. A contradiction. Hence the word  $w$  synchronizes the automaton  $\mathcal{D}^{ab}(q, p, k)$  to the state  $q - p + 1$ .

The proof of the part (ii) of the lemma is analogous to the part (i) with only minor changes.

**Theorem 4.** *The reset threshold of the Dulmage-Mendelsohn-type automaton  $\mathcal{D}^{ab}(q, p, k)$  is equal to  $(p-1)(q-1) + q - p - k$ .*

*Proof.* Let  $w$  be a reset word for the automaton  $\mathcal{D}^{ab}(q, p, k)$  having minimal length. By lemma 5 the word  $w$  synchronizes the automaton to the state  $q - p + 1$ . Note, that any word of length  $q - p - k$  brings the state  $k + 1$  to the state  $q - p + 1$ . Lemma 1 implies  $|w| \geq (p-1)(q-1) + q - p - k$ .

First let us assume that  $k = q - p$ . In this case it remains to prove that the word  $w_1 = (ba^{q-1})^{p-2}ba^{q-p}$  is synchronizing. Let  $C$  be the cycle  $\{0, q - p + 1, q - p + 2, \dots, q - 1\}$ . Note, that the word  $ba^{q-1}$  maps all the states, that do not belong to  $C$ , to the set  $C \cdot ba^{q-1}$ . Namely,  $k \cdot ba^{q-1} = (t-1) \cdot ba^{q-1}$ , where  $t = k \cdot b$ ;  $(k-1) \cdot ba^{q-1} = (q-1) \cdot ba^{q-1}$ ,  $(k-2) \cdot ba^{q-1} = (q-2) \cdot ba^{q-1}, \dots, 1 \cdot ba^{q-1} = (q-k+1 = p+1) \cdot ba^{q-1}$ . Thus it is enough to consider the action of the word  $w_1$  on the cycle  $C$ . By lemma 2 we have  $C \cdot (ba^{q-1})^{p-2} = \{0, q - r\}$ , where

$r$  is the remainder of the division of  $q$  by  $p$ . But then it is easy to see, that  $0.ba^{q-p} = (q-r).ba^{q-p} = q-p+1$ .

Now assume that  $k < q-p$ . Let us show that the word

$$w_2 = ba^{q-p-k-1}(ba^{q-1})^{p-2}ba^{q-p}$$

is synchronizing. All the states in the range from  $k$  to  $q-p$  are mapped into the cycle  $C$  under the action of the prefix  $ba^{q-p-k-1}$ . This prefix maps the remaining states lying outside the cycle  $C$ , i.e.  $1, 2, \dots, k-1$ , to the states ranging from  $q-p-k+1$  to  $q-p-1$ . Namely,  $(k-i).ba^{q-p-k-1} = q-p-i$  for  $1 \leq i \leq k-1$ . The action of the word  $ba^{q-1}$  on the states in  $\{q-p-k+1, \dots, q-p-1\}$  coincides with the action of this word on some states in the cycle  $C$ . More precisely, we have  $(q-p-i).ba^{q-1} = (q-i).ba^{q-1}$  for  $1 \leq i \leq k-1$ , provided that for no such  $i$  we have  $q-p-i = k$ . If  $q-p-i = k$  for some  $i$ , then we have  $k.ba^{q-1} = (t-1).ba^{q-1}$ , where  $t = k.b$ . In both cases the condition  $k < p$  implies that all the resulting states  $t-1, q-1, \dots, q-k+1$  lie on the cycle  $C$ . Hence the word  $w_2$  brings the automaton  $\mathcal{D}^{ab}(q, p, k)$  into the subset of  $C.(ba^{q-1})^{p-2}ba^{q-p}$ . As we have already seen, the latter set is the singleton  $q-p+1$ .

**Theorem 5.** *The reset threshold of the Dulmage-Mendelsohn-type automaton  $\mathcal{D}^{aa}(q, p, k)$  equals  $(p-1)(q-1) + q-p-k$  if  $k < q-p$ , and  $(p-1)(q-1) + 2(q-p)$  if  $k = q-p$ .*

*Proof.* First let us assume that  $k < q-p$ . Let  $w$  be reset word for the automaton  $\mathcal{D}^{aa}(q, p, k)$  having minimal possible length. Lemma 5 implies that the word  $w$  brings the automaton to the state  $q-p+1$ . Note, that any word of length  $q-p-k$  brings the state  $k+1$  to the state  $q-p+1$ . Thus by lemma 1 we have  $|w| \geq (p-1)(q-1) + q-p-k$ .

Let us prove that the word  $w_1 = a^{q-p-k}(ba^{k-1}ba^{q-k-1})^{p-2}ba^{k-1}ba^{q-p-k}$  is synchronizing. Consider the cycle  $C = \{0, q-p+1, q-p+2, \dots, q-1\}$ . Note, that the prefix  $a^{q-p-k}$  maps the states, ranging from  $k+1$  to  $q-p$ , to the states in  $C$ . Consider now the action of the prefix  $a^{q-p-k}$  on the states from 1 to  $k$ . If  $q-p-k+1 > k$ , then all these states are mapped to some states in  $C$ . If  $q-p-k+1 \leq k$ , then these states are mapped into  $C \cup \{q-p-k+1, \dots, k\}$ . Next, for each state  $t$  from  $q-p-k+1$  to  $k$  we present a state  $t'$  from  $C$  such that  $t.ba^{k-1} = t'.ba^{k-1}$ . If  $t \neq k$ , then it is easy to check that  $t' = q-p+t$ . Since  $q-p-k+1 > 1$ , we have  $t' > q-p+1$ . Hence the state  $t' \in C$ . If  $t = k$ , then  $t' = k+p$  (recall, that  $k+p < q$ ). The state  $k+p$  belongs to  $C$ . Indeed, from  $q-p-k+1 \leq k$  and  $k < p$  we obtain  $k+p > 2k \geq q-p+1$ . Hence the word  $w_1$  brings the automaton  $\mathcal{D}^{aa}(q, p, k)$  into the subset of  $C.(ba^{k-1}ba^{q-k-1})^{p-2}ba^{k-1}ba^{q-p-k}$ . Thus it remains to show, that the latter set is a singleton. The argument is similar to the proof of lemma 2. Instead of the word  $ba^{q-1}$  we use the word  $v = ba^{k-1}ba^{q-k-1}$ . First we note, that the word  $v$  fixes the state 0. The word  $v$  moves all the other states in  $C$  except  $q-k$  along the cycle in the same way as the word  $ba^{q-1}$  does in lemma 2. The state  $q-k$  leaves the cycle after applying the prefix  $ba^{k-1}b$ , but it can be easily seen that

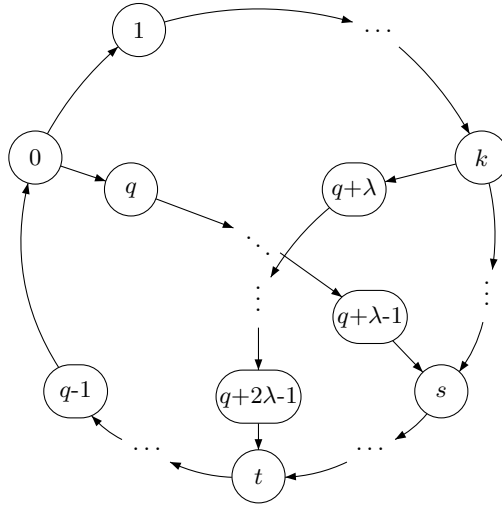


$(q-k) \cdot ba^{k-1}ba^{q-k-1} = (q-k) \cdot ba^{k-1}aa^{q-k-1}$ . Thus we may treat the state  $q-k$  as if it never left the cycle  $C$ . Following the argument in lemma 2, we conclude, that  $C \cdot v^{p-2} = \{0, q-r\}$ , where  $r$  is the remainder of the division of  $q$  by  $p$ . Finally, we observe that  $0 \cdot ba^{k-1}ba^{q-p-k} = (q-r) \cdot ba^{k-1}ba^{q-p-k} = q-p+1$ .

Consider now the case  $k = q-p$ . Let  $w$  be a synchronizing word for the automaton  $\mathcal{D}^{aa}(q, p, k)$  having minimal possible length. Since the incoming edges to the state  $q-p+1$  have different labels, the word  $w$  necessarily resets the automaton to the state  $q-p+1+k$ . For convenience, let  $t$  denote the state  $q-p+1+k$ . Every word of length  $k$  brings the state  $q-p+1$  to the state  $t$ . Therefore, by lemma 1 we have  $|w| \geq (p-1)(q-1) + k$ . Suppose  $|w| = (p-1)(q-1) + k + i$  for some  $0 \leq i \leq k-1$ . Consider the states  $q-i$  (the state 0, if  $i = 0$ ) and  $q-p-i$ . The prefix of  $w$  of length  $k+1+i$  will bring one of these states to the state  $t$  depending on the  $(i+1)$ st letter. The remaining  $(p-1)(q-1) - 1$  letters of  $w$  will move the state  $t$  to itself. But this path is a combination of cycles of lengths  $p$  and  $q$ , which is impossible by theorem 1. Consequently,  $|w| \geq (p-1)(q-1) + 2k = (p-1)(q-1) + 2(q-p)$ .

Let us prove that the word  $w_2 = a^{q-p}(ba^{k-1}ba^{q-k-1})^{p-2}ba^{k-1}ba^{q-p}$  is synchronizing. The prefix  $a^{q-p}$  brings all the states lying outside the cycle  $C = \{0, q-p+1, q-p+2, \dots, q-1\}$  into  $C$ . Arguing as in the previous case we conclude, that  $C \cdot (ba^{k-1}ba^{q-k-1})^{p-2} = \{0, q-r\}$ . It is easy to see, that  $0 \cdot ba^{k-1}ba^{q-p} = (q-r) \cdot ba^{k-1}ba^{q-p} = t$ .

We can partially generalize this result as we did in theorem 3 for the case of more than  $q$  states. We consider a primitive digraph  $D_\lambda(q, p, k)$  presented on Fig. 5, where  $1 \leq \lambda < p$ . For convenience, we set  $D_0(q, p, k) = D(q, p, k)$ . Its colorings are denoted by  $\mathcal{D}_\lambda^{aa}(q, p, k)$  and  $\mathcal{D}_\lambda^{ab}(q, p, k)$ .



**Fig. 5.** The digraph  $D_\lambda(q, p, k)$

**Lemma 6.** *If  $1 \leq \lambda < p$  and  $z \in \{a, b\}$ , then  $\mathcal{D}_\lambda^{az}(q, p, k)/\sigma$  is equal to  $\mathcal{D}_{\lambda-1}^{az}(q, p, k)$ , and*

$$\text{rt}(\mathcal{D}_\lambda^{az}(q, p, k)) = \text{rt}(\mathcal{D}_{\lambda-1}^{az}(q, p, k)) + 1.$$

*Proof.* Let  $w$  be a word synchronizing the automaton  $\mathcal{D}_\lambda^{az}(q, p, k)$  having minimal length. Then  $w$  resets the automaton either to the state  $s$ , or to the state  $t$ . Let  $x$  be the last letter of  $w$ , so that  $w = w'x$ . The word  $w'$  brings the automaton  $\mathcal{D}_\lambda^{az}(q, p, k)$  either to the set  $\{q + \lambda - 1, s - 1\}$ , or  $\{q + 2\lambda - 1, t - 1\}$ . These two pairs of states form the two non-trivial  $\sigma$ -classes. Hence the factor automaton  $\mathcal{D}_\lambda^{az}(q, p, k)/\sigma$  is equal to  $\mathcal{D}_{\lambda-1}^{az}(q, p, k)$ , and it is synchronized by  $w'$ . Thus  $\text{rt}(\mathcal{D}_\lambda^{az}(q, p, k)/\sigma) \leq \text{rt}(\mathcal{D}_{\lambda-1}^{az}(q, p, k)) - 1$ . On the other hand, by lemma 3 we have  $\text{rt}(\mathcal{D}_\lambda^{az}(q, p, k)/\sigma) \geq \text{rt}(\mathcal{D}_{\lambda-1}^{az}(q, p, k)) - 1$ , and we get the required equality.

**Theorem 6.** *If  $1 \leq \lambda < p$ , then*

- (i)  $\text{rt}(\mathcal{D}_\lambda^{ab}(q, p, k)) = (p - 1)(q - 1) + q - p - k + \lambda$ ;
- (ii)  $\text{rt}(\mathcal{D}_\lambda^{aa}(q, p, k)) = (p - 1)(q - 1) + q - p - k + \lambda$ , if  $k < q - p$ ;
- (iii)  $\text{rt}(\mathcal{D}_\lambda^{aa}(q, p, k)) = (p - 1)(q - 1) + 2(q - p) + \lambda$ , if  $k = q - p$ .

*Proof.* Since there are  $\lambda$  states both on the path from the state 0 to  $s$ , and from  $k$  to  $t$ , and  $k \leq k - p$ , lemma 6 can be applied  $\lambda$  times. Each time lemma 6 is applied, the reset threshold is decreased strictly by one. In the end, from the automaton  $\mathcal{D}_\lambda^{ab}(q, p, k)$  we obtain the automaton  $\mathcal{D}_0^{aa}(q, p, k)$ , whose reset threshold is known by theorem 4. Therefore, we have  $\text{rt}(\mathcal{D}_\lambda^{ab}(q, p, k)) = (p - 1)(q - 1) + q - p - k + \lambda$ . In an analogous way from the automaton  $\mathcal{D}_\lambda^{aa}(q, p, k)$  we obtain the automaton  $\mathcal{D}_0^{aa}(q, p, k)$ . Applying theorem 5, we obtain  $\text{rt}(\mathcal{D}_\lambda^{aa}(q, p, k)) = (p - 1)(q - 1) + q - p - k + \lambda$  in case  $k < q - p$ , and  $\text{rt}(\mathcal{D}_\lambda^{aa}(q, p, k)) = (p - 1)(q - 1) + 2(q - p) + \lambda$  if  $k = q - p$ .

The case of non-equal number of states on the paths from 0 to  $s$  and from  $k$  to  $t$  is much more technical, and will be published elsewhere.

## References

1. Ananichev, D. S., Gusev, V. V., Volkov M. V. *Primitive digraphs with large exponents and slowly synchronizing automata*. Journal of Mathematical Sciences (US), 192(3), 263–278 (2013).
2. Ananichev, D. S., Volkov, M. V., Zaks, Yu. I. *Synchronizing automata with a letter of deficiency 2*. Theor. Comput. Sci., 376, 30–41 (2007).
3. Brualdi R., Ryser H. *Combinatorial matrix theory*. Cambridge University Press, (1991).
4. Černý, J. *Poznámka k homogénnym experimentom s konečnými automatami*. Mat.-Fyz. Cas. Slovensk. Akad. Vied., 14 208–216 (1964).
5. Dulmage A. L., Mendelsohn N. S. *Gaps in the exponent set of primitive matrices*. Illinois J. Math., 8(4), 642–656 (1964).
6. Kisielewicz A., Szykua M. *Generating Small Automata and the ern Conjecture*. Proc. of CIAA 2013. Lect. Notes Comp. Sci., 7982, 340–348 (2013).
7. Lewin, M., Vitek, Y. *A system of gaps in the exponent set of primitive matrices*. Illinois J. Math., 25, 87–98 (1981).

8. Pin, J.-E. *On two combinatorial problems arising from automata theory*. Ann. Discrete Math., 17, 535–548 (1983).
9. Ramírez Alfonsín, J.L. *The diophantine Frobenius problem*. Oxford University Press (2005)
10. Sandberg S. *Homing and synchronizing sequences*. In M. Broy et al (eds.) Model-Based Testing of Reactive Systems, Lect. Notes Comput. Sci., **3472**, 5–33 (2005).
11. Trahtman A.N. *Notable trends concerning the synchronization of graphs and automata*. Electr. Notes Discrete Math., 25, 173–175 (2006).
12. Trahtman A.N. *The Road Coloring Problem*. Israel J. Math., 172, 51–60 (2009).
13. Volkov M.V. *Synchronizing automata and the Černý conjecture*. Proc. of LATA 2008. Lect. Notes Comp. Sci., **5196**, 11–27 (2008).